Amendments to the Claims:

The following listing of claims replace all prior listings.

Listing Of Claims:

1-5. (Cancelled)

6. (Currently Amended) A method, comprising:

determining, in a first network, an address associated with a called party of a second network;

determining based on said address if said called party is in a trusted network, wherein the determining if the called party is in a trusted network comprises checking if the address is contained in a database of trusted networks provided in at least one of a serving call session control function [[or]] and a security gateway; and

controlling communication between the called party and a calling party of the first network based on if said called party is in the trusted network, the communication comprising at least one message for the called party, wherein if the called party is not in the trusted network, the controlling comprises modifying the at least one message, wherein controlling is performed by at least one processor.

7. (Currently Amended) A method, comprising:

determining, in a first network, an address associated with a called party of a second network;

determining based on said address if said called party is in a trusted network, wherein the determining if the called party is in a trusted network comprises checking if

the address is contained in a database of trusted networks, wherein said database comprises domain names associated with the trusted networks and internet protocol addresses of the trusted networks; and

controlling communication between the called party and a calling party of the first network based on if said called party is in the trusted network, the communication comprising at least one message for the called party, wherein if the called party is not in the trusted network the controlling compromises modifying the at least one message, wherein controlling is performed by at least one processor.

8. (Cancelled)

9. (Currently Amended) A method, comprising:

determining, in a first network, an address associated with a called party of a second network;

determining based on said address if said called party is in a trusted network, wherein said determining, in the first network, the address comprises determining if the address contains a domain name, wherein if a determination is made that the address does not contain the domain name, the determining, in the first network, the address comprises sending a request for the domain name; and

controlling communication between the called party and a calling party of the first network based on if said called party is in the trusted network, the communication comprising at least one message for the called party, wherein if the called party is not in the trusted network, the controlling comprises modifying the at least one message, wherein controlling is performed by at least one processor.

10. (Previously Presented) The method as claimed in claim 9, wherein the determining, in the first network, the address comprises sending said request to a domain name server.

11. (Currently Amended) A method, comprising:

determining, in a first network, an address associated with a called party of a second network;

determining based on said address if said called party is in a trusted network, wherein said determining, in the first network, the address comprises determining if the address contains a domain name, wherein if a determination is made that the address does not contain the domain name, the determining, in the first network, the address comprises assuming that the called party is in an untrusted network; and

controlling communication between the called party and a calling party of the first network based on if said called party is in the trusted network, the communication comprising at least one message for the called party, wherein if the called party is not in the trusted network, the controlling comprises modifying the at least one message, wherein controlling is performed by at least one processor.

12-17. (Cancelled)

18. (Currently Amended) The method as claimed in claim [[17]]6, wherein the determining if the called party is in the trusted network ~~is performed in a gateway of the~~

~~calling network~~ further comprises determining if a connection from a calling network to a called network is secured.

19. (Currently Amended) The method as claimed in claim [[18]]7, wherein the determining if the called party is in the trusted network further comprises determining if ~~the connection between the gateway of the calling network and a gateway of the called network comprises a secure connection~~ a connection from a calling network to a called network is secured.

20-35. (Cancelled)

36. (Currently Amended) An apparatus, comprising:

a first determiner configured to determine an address associated with a called party located in another network;

a second determiner configured to determine, based on said address, if said called party is in a trusted network, wherein the second determiner is further configured to check if the address is contained in a database of trusted networks, wherein the database is provided in at least one of a serving call session control function [[or]] and a security gateway; and

a controller configured to control communication between the called party and a calling party, located in a network where the apparatus is located, based on if said

called party is in the trusted network, the communication comprising at least one message for the called party, wherein if the called party is not in the trusted network, the at least one message for the called party is modified.

37. (Previously Presented) An apparatus, comprising:

a first determiner configured to determine an address associated with a called party located in another network;

a second determiner configured to determine, based on said address, if said called party is in a trusted network, the second determiner being configured to check if the address is contained in a database of trusted networks, wherein said database comprises domain names associated with the trusted networks and internet protocol addresses of the trusted networks; and

a controller configured to control communication between the called party and a calling party, located in a network where the apparatus is located, based on if said called party is in the trusted network, the communication comprising at least one message for the called party, wherein if the called party is not in the trusted network, the at least one message for the called party is modified.

38. (Cancelled)

39. (Previously Presented) An apparatus, comprising:

a first determiner configured to determine an address associated with a called party located in another network;

a second determiner configured to determine, based on said address, if said called party is in a trusted network, wherein the first determiner is further configured to determine if the address contains a domain name, wherein if a determination is made that the address does not contain the domain name, the first determiner is further configured to send a request for the domain name; and

a controller configured to control communication between the called party and a calling party, located in a network where the apparatus is located, based on if said called party is in the trusted network, the communication comprising at least one message for the called party, wherein if the called party is not in the trusted network, the at least one message for the called party is modified.

40. (Previously Presented) The apparatus as claimed in claim 39, wherein the first determiner is further configured to send said request to a domain name server.

41. (Previously Presented) An apparatus, comprising:

a first determiner configured to determine an address associated with a called party located in another network;

a second determiner configured to determine, based on said address, if said called party is in a trusted network, wherein the first determiner is further configured to

determine if the address contains a domain name, wherein if a determination is made that the address does not contain the domain name, the first determiner is further configured to assume that the called party is in an untrusted network; and

a controller configured to control communication between the called party and a calling party, located in a network where the apparatus is located, based on if said called party is in the trusted network, the communication comprising at least one message for the called party, wherein if the called party is not in the trusted network, the at least one message for the called party is modified.

42-45. (Cancelled)

46. (Currently Amended) The apparatus as claimed in claim [[45]]36~~, further comprising a gateway of the calling network~~, wherein the determining if the called party is in the trusted network further comprises determining if a connection from a calling network to a called network is secured.

47. (Currently Amended) The apparatus as claimed in claim [[45]]37~~, wherein the gateway of the called network comprises a secure connection~~ wherein the determining if the called party is in the trusted network further comprises determining if a connection from a calling network to a called network is secured.

48-52. (Cancelled)

53. (Currently Amended) A method comprising:

determining at a serving call session control function in an internet protocol multimedia subsystem network a trust relation with a called party in another network, wherein the determining if the called party is in a trusted relationship comprises checking a database of trusted networks provided in at least one of a serving call session control function [[or]] and a security gateway; and

controlling communication of a message to the called party based on the determination, wherein if the called party is not trusted the call session control function removes identity information relating to the calling party from the message, and if the called party is trusted said identity information is retained, wherein controlling is performed by at least one processor.

54. (Canceled)

55. (Cancelled)